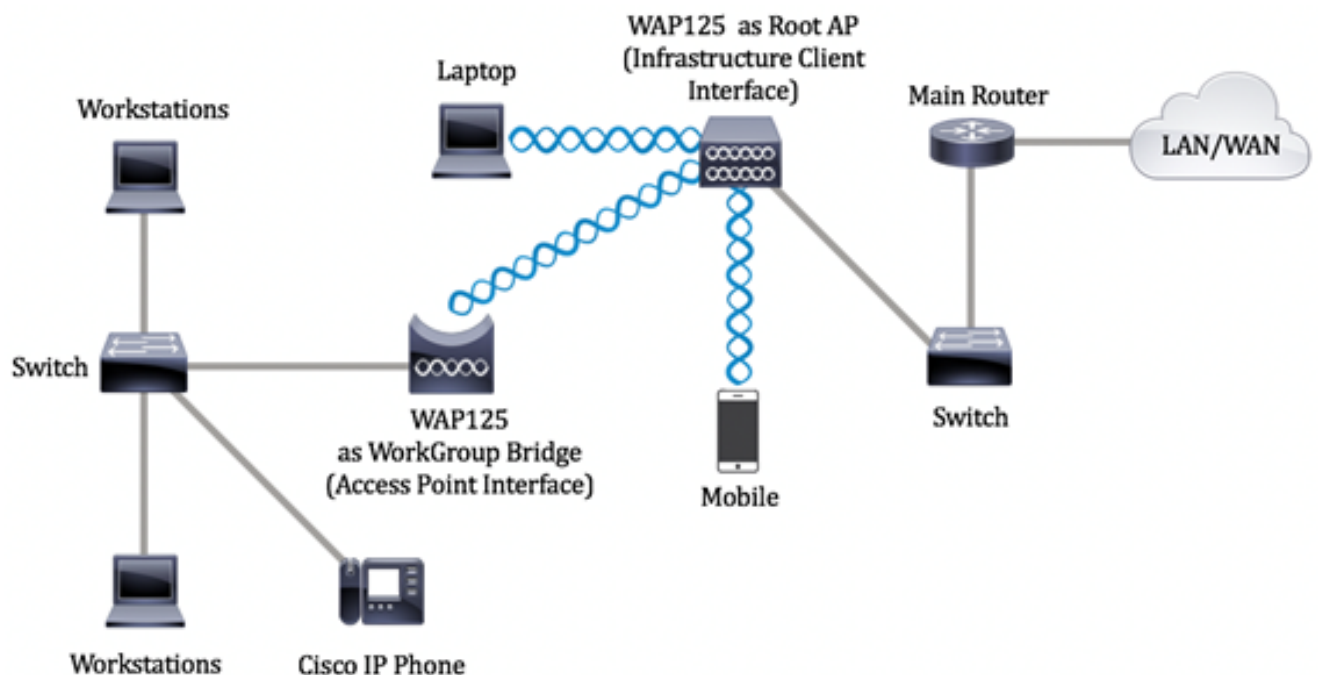


Definir as configurações de ligação do grupo de trabalho nos pontos de acesso WAP125 ou WAP581

Objetivo

O recurso WorkGroup Bridge permite que o Ponto de Acesso Sem Fio (WAP - Wireless Access Point) faça a ponte do tráfego entre um cliente remoto e a LAN (Local Area Network) sem fio conectada ao Modo de Bridge do Grupo de Trabalho. O dispositivo WAP associado à interface remota é conhecido como uma interface de ponto de acesso, enquanto o dispositivo WAP associado à LAN sem fio é conhecido como uma interface de infraestrutura. A ligação de grupo de trabalho permite que os dispositivos que têm ligações com fios se conectem a uma rede sem fios. O modo de bridge para grupo de trabalho é recomendado como uma alternativa quando o recurso Wireless Distribution System (WDS) não está disponível.

A topologia abaixo ilustra um exemplo de modelo de ligação de grupo de trabalho. Os dispositivos com fio são ligados a um switch, que se conecta à interface LAN do WAP. No exemplo abaixo, o WAP125 atua como uma interface de ponto de acesso que se conecta à interface do cliente de infraestrutura.



Este artigo fornece instruções sobre como configurar a ligação de grupo de trabalho entre dois pontos de acesso sem fio.

Dispositivos aplicáveis

- WAP125
- WAP581

Versão de software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Definir as configurações da ponte do grupo de trabalho

Antes de configurar o Work Group Bridge no dispositivo WAP, observe estas diretrizes:

- Todos os dispositivos WAP que participam do WorkGroup Bridge devem ter as seguintes configurações idênticas:
 - Rádio
 - Modo IEEE 802.11
 - Largura de banda do canal
 - Canal (Auto não é recomendado)

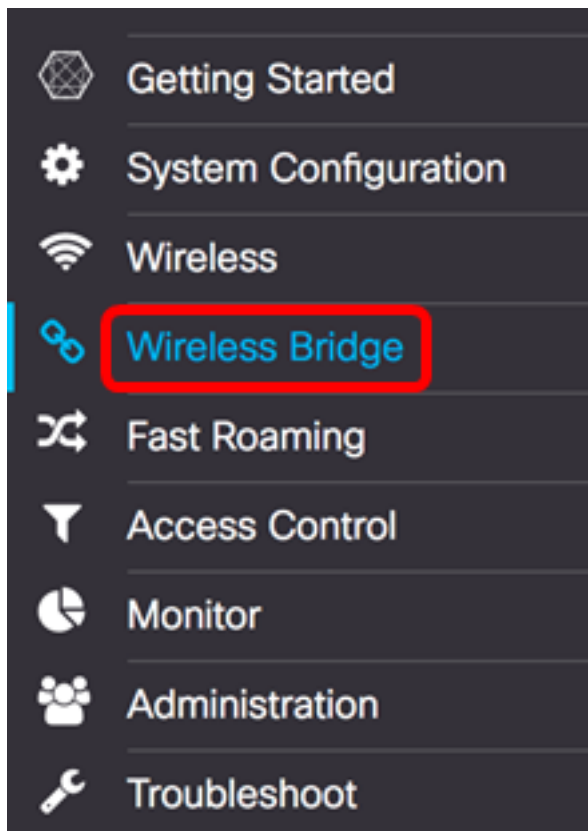
Note: Para saber como definir essas configurações no WAP125, clique [aqui](#) para obter instruções. Para WAP581, clique [aqui](#).

- O modo de ligação de grupo de trabalho suporta atualmente apenas o tráfego IPv4.
- O modo de ligação de grupo de trabalho não é suportado através de uma configuração de ponto único. Se você tiver pontos de acesso WAP581, desabilite a SPS ou o clustering primeiro antes de definir as configurações da ligação do grupo de trabalho. Para obter instruções sobre como configurar as configurações de SPS em seu WAP, clique [aqui](#).

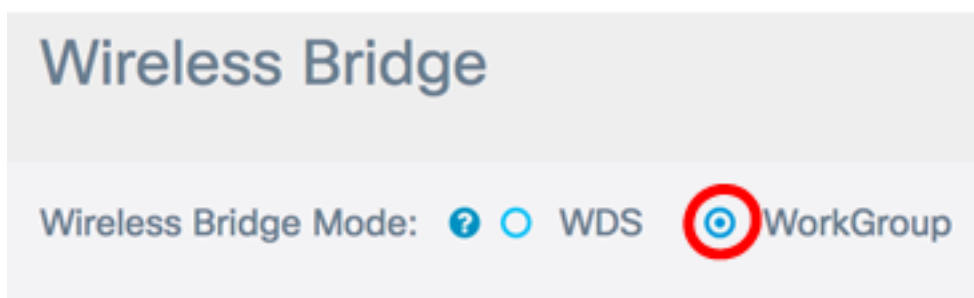
Configurar a interface do cliente de infraestrutura

Etapa 1. Faça login no utilitário baseado na Web do WAP e escolha **Wireless Bridge**.

Note: As opções disponíveis podem variar dependendo do modelo exato do dispositivo. Neste exemplo, WAP125 é usado.



Etapa 2. Clique no botão de opção **Grupo de trabalho**.



Etapa 3. Marque a caixa de seleção **Uplink**.

	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Etapa 4. Clique no ícone **Editar**.



<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Etapa 5. Marque a caixa de seleção **Habilitado** para habilitar a interface do cliente de infraestrutura.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input checked="" type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)

Etapa 6. Escolha a interface de rádio para o WorkGroup Bridge. Quando você configura um rádio como uma ligação de grupo de trabalho, o outro rádio permanece operacional. As interfaces de rádio correspondem às bandas de radiofrequência do WAP. O WAP está equipado para transmitir em duas interfaces de rádio diferentes. A definição das configurações de uma interface de rádio não afetará a outra.

Enabled	Radio
<input checked="" type="checkbox"/>	<input type="text" value="Radio 1 (2.4 GHz)"/> <input checked="" type="text" value="Radio 2 (5 GHz)"/>

Note: Neste exemplo, a opção Radio 2 (5 GHz) é escolhida.

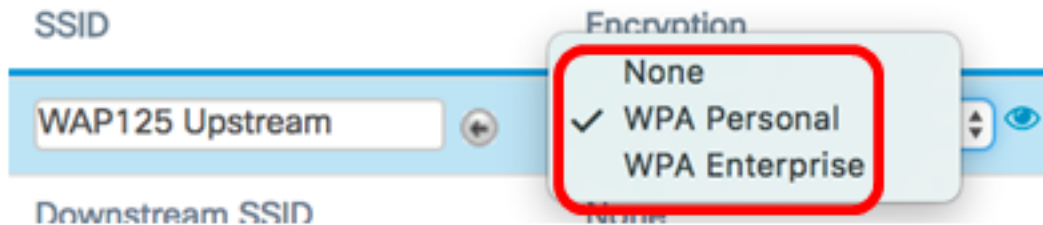
Passo 7. Insira o nome do SSID (Service Set Identifier, Identificador do conjunto de serviços) no campo *SSID*. Isso serve como a conexão entre o dispositivo e o cliente remoto. Você pode digitar de 2 a 32 caracteres para o SSID do cliente de infraestrutura.

Note: Neste exemplo, é usado o Upstream WAP125.

Radio	SSID
<input type="text" value="Radio 2 (5 GHz)"/>	<input type="text" value="WAP125 Upstream"/>


Note: A seta ao lado do SSID está disponível para a digitalização do SSID. Esse recurso é desabilitado por padrão e é habilitado somente se a Detecção de AP estiver habilitada na Detecção de AP não autorizado, que também é desabilitada por padrão.

Etapa 8. Escolha o tipo de segurança para autenticar como uma estação cliente no dispositivo WAP de upstream na lista suspensa Criptografia. As opções são:



- Nenhum — Aberto ou sem segurança. Esse é o padrão. Se isso for escolhido, vá para a [Etapa 22](#).
- WPA Personal — A WPA Personal pode suportar chaves com 8 a 63 caracteres. A WPA2 é recomendada porque tem um padrão de criptografia mais potente.
- WPA Enterprise — A WPA Enterprise é mais avançada que a WPA Personal e é a segurança recomendada para autenticação. Usa o PEAP (Protected Extensible Authentication Protocol) e o TLS (Transport Layer Security). Vá para a [Etapa 12](#) para configurar. Esse tipo de segurança é frequentemente usado em um ambiente de escritório e precisa de um servidor RADIUS (Remote Authentication Dial-In User Service) configurado. Clique [aqui](#) para saber mais sobre os servidores RADIUS.

Note: Neste exemplo, a WPA Personal é escolhida.

Etapa 9. Clique no  ícone e marque a caixa de seleção WPA-TKIP ou WPA2-AES para determinar que tipo de criptografia WPA a interface do cliente de infraestrutura usará.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Note: Se todos os seus equipamentos sem fio oferecerem suporte a WPA2, defina a segurança do cliente da infraestrutura como WPA2-AES. O método de criptografia é RC4 para WPA e AES (Advanced Encryption Standard) para WPA2. A WPA2 é recomendada porque tem um padrão de criptografia mais potente. Neste exemplo, WPA2-AES é usado.

Etapa 10. (Opcional) Se você marcou o WPA2-AES na Etapa 9, escolha uma opção na lista suspensa Proteção de Quadro de Gerenciamento (MFP) se deseja que o WAP exija quadros protegidos ou não. Para saber mais sobre o MFP, clique [aqui](#). As opções são:

- Não obrigatório — Desativa o suporte ao cliente para MFP.
- Capable (Capaz) — Permite que clientes compatíveis com MFP e que não suportam MFP entrem na rede. Essa é a configuração MFP padrão no WAP.
- Obrigatório — Os clientes podem se associar somente se o MFP for negociado. Se os dispositivos não oferecerem suporte a MFP, eles não poderão ingressar na rede.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

Note: Neste exemplo, Capable é escolhido.

Etapa 11. Insira a chave de criptografia WPA no campo *Key (Chave)*. A chave deve ter de 8 a 63 caracteres. É uma combinação de letras, números e caracteres especiais. É a senha usada ao conectar-se à rede sem fio pela primeira vez. Então, vá para a [Etapa 21](#).

MFP:

Key:

Show Key as Clear Text

[Etapa 12](#). Se você escolheu WPA Enterprise na Etapa 8, clique em um botão de opção para o Método EAP.

As opções disponíveis são definidas da seguinte forma:

- PEAP — Este protocolo fornece a cada usuário sem fio nomes de usuário e senhas individuais WAP que suportam padrões de criptografia AES. Como o PEAP é um método de segurança baseado em senha, a segurança Wi-Fi baseia-se nas credenciais do dispositivo do cliente. O PEAP pode representar um risco de segurança potencialmente grave se você tiver senhas fracas ou clientes não protegidos. Ele depende do TLS, mas evita a instalação de certificados digitais em todos os clientes. Em vez disso, ele fornece autenticação através de um nome de usuário e senha.
- TLS — O TLS exige que cada usuário tenha um certificado adicional para ter acesso. O TLS é mais seguro se você tiver os servidores adicionais e a infraestrutura necessária para autenticar usuários na sua rede. Se você escolher essa opção, vá para a [Etapa 14](#).

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Note: Para este exemplo, PEAP é escolhido.

Etapa 13. Insira o nome de usuário e a senha do cliente de infraestrutura nos campos Nome de usuário e Senha. Essas são as informações de login usadas para conectar-se à interface do cliente da infraestrutura; consulte a interface do seu cliente de infraestrutura para encontrar essas informações. Então, vá para a [Etapa 21](#).

EAP Method: PEAP TLS

Username:

Password:

Show Key as Clear Text

[Etapa 14](#). Se você clicou em TLS na Etapa 12, insira a identidade e a chave privada do cliente de infraestrutura nos campos Identidade e Chave privada.

EAP Method: PEAP TLS

Identity:

Private Key:

Show Key as Clear Text

Etapa 15. Na área do método de transferência, clique em um botão de opção das seguintes opções:

- TFTP — O TFTP (Trivial File Transfer Protocol) é uma versão simplificada e não segura do FTP. É usado principalmente para distribuir software ou autenticar dispositivos entre redes corporativas. Se você clicou em TFTP, vá para a [Etapa 18](#).
- HTTP — O HTTP (Hypertext Transfer Protocol) fornece uma estrutura de autenticação de desafio-resposta simples que pode ser usada por um cliente para fornecer a estrutura de autenticação.

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Note: Se um arquivo de certificado já estiver presente no WAP, os campos Arquivo de certificado presente e Data de expiração do certificado já serão preenchidos com as informações relevantes. Caso contrário, estarão em branco.

HTTP

Etapa 16. Clique no botão **Procurar** para localizar e selecionar um arquivo de certificado. O arquivo deve ter a extensão de arquivo de certificado adequada (como .pem ou .pfx); caso contrário, o arquivo não será aceito.



Note: Neste exemplo, Certificate.pfx é escolhido.

Etapa 17. Clique em **Carregar** para carregar o arquivo de certificado selecionado. Vá para a [Etapa 21](#).

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: Certificate.pfx

Os campos Arquivo de certificado presente e Data de expiração do certificado serão atualizados automaticamente.

TFTP

[Etapa 18](#). (Opcional) Se você clicou em TFTP na Etapa 15, insira o nome do arquivo de certificado no campo *Nome do arquivo*.

Transfer Method: HTTP TFTP

Filename

Note: Neste exemplo, Certificate.pfx é usado.

Etapa 19. Insira o endereço do servidor TFTP no campo *Endereço IPv4 do servidor TFTP*.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Note: Neste exemplo, 192.168.100.108 é usado como o endereço do servidor TFTP.

Etapa 20. Clique no botão **Carregar** para carregar o arquivo de certificado especificado.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Os campos Arquivo de certificado presente e Data de expiração do certificado serão atualizados automaticamente.

[Etapa 21.](#) Clique em **OK** para fechar a janela Security Setting (Configuração de segurança).

A área Status da conexão indica se o WAP está conectado ao dispositivo WAP de upstream.

Encryption	Connection Status
<input type="text" value="WPA Personal"/>	<input type="text" value="Disconnected"/>

[Etapa 22.](#) Digite a ID da VLAN para a interface do cliente de infraestrutura. O padrão é 1.

Connection Status	VLAN ID
<input type="text" value="Disconnected"/>	<input type="text" value="1"/>

Note: Para este exemplo, o ID de VLAN padrão é usado.

Etapa 23. Clique em **Salvar** para salvar as configurações definidas.

Save

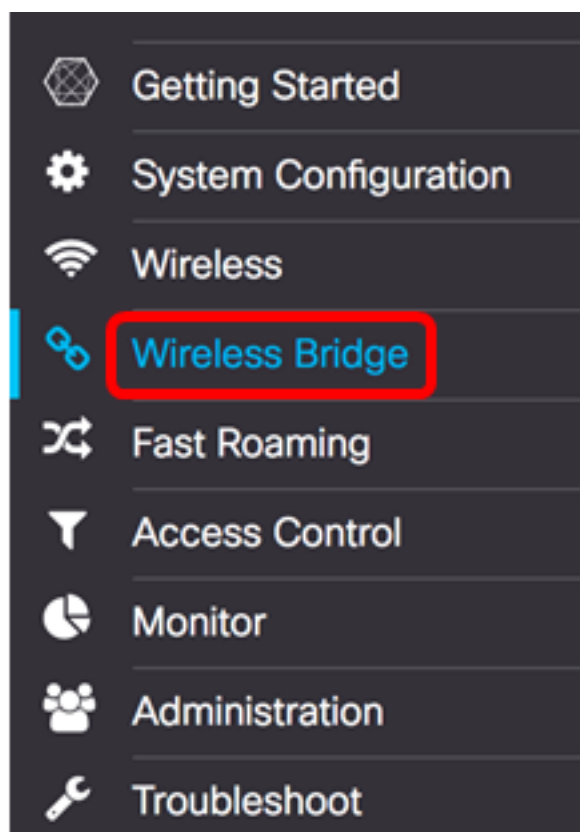
Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	<input type="text" value="1"/>	N/A	N/A
N/A	1	<input checked="" type="checkbox"/>	Disabled

Agora você deve ter configurado com êxito as configurações da interface do cliente de infraestrutura em seu WAP.

Configurar a interface do cliente do ponto de acesso

Etapa 1. Faça login no utilitário baseado na Web do WAP e escolha **Wireless Bridge**.

Note: As opções disponíveis podem variar dependendo do modelo exato do dispositivo. Neste exemplo, WAP125 é usado.



Etapa 2. Clique no botão de opção **Grupo de trabalho**.

Wireless Bridge

Wireless Bridge Mode: ? WDS WorkGroup

Etapa 3. Marque a caixa de seleção **Downlink**.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Etapa 4. Clique no botão **Editar**.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Etapa 5. Marque a caixa de seleção **Habilitado** para habilitar o bridging na interface do ponto de acesso.

<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
-------------------------------------	----------	-------------------------------------	-----------------

Etapa 6. Digite o SSID do ponto de acesso no campo *SSID*. O comprimento do SSID deve estar entre 2 e 32 caracteres. O padrão é Downstream SSID.

Radio 2 (5 GHz)	WAP125 Downstream
-----------------	-------------------

Note: Para este exemplo, o SSID usado é WAP125 Downstream.

Passo 7. Escolha o tipo de segurança para autenticar estações clientes downstream para o WAP na lista suspensa Segurança.

As opções disponíveis são definidas da seguinte forma:

- Nenhum — Aberto ou sem segurança. Este é o valor padrão. Vá para a [Etapa 13](#) se

escolher esta opção.

- WPA Personal — A WPA (Wi-Fi Protected Access) Personal pode suportar chaves com 8 a 63 caracteres. O método de criptografia é TKIP ou Counter Cipher Mode com Block Chaining Message Authentication Code Protocol (CCMP). A WPA2 com CCMP é recomendada porque tem um padrão de criptografia mais potente, o AES (Advanced Encryption Standard), em comparação com o TKIP (Temporal Key Integrity Protocol) que usa apenas um padrão RC4 de 64 bits.



Etapa 8. (Opcional) Marque a caixa de seleção WPA-TKIP para determinar a criptografia WPA-TKIP que a interface do ponto de acesso usará. Isso está habilitado por padrão.

Note: O WPA-AES está acinzentado e não pode ser desativado. Neste exemplo, WPA-TKIP está desmarcada.

Security Setting

WPA Versions:

WPA-TKIP WPA2-AES

Etapa 9. Insira a chave WPA compartilhada no campo Key (Chave). A chave deve ter de 8 a 63 caracteres e pode incluir caracteres alfanuméricos, letras maiúsculas e minúsculas e caracteres especiais.

WPA Versions:

WPA-TKIP WPA2-AES

Key: ?

.....

Show Key as Clear Text

Etapa 10. Insira a taxa no campo Broadcast Key Refresh Rate (Taxa de atualização da chave de transmissão). A taxa de atualização da chave de broadcast especifica o intervalo no qual a chave de segurança é atualizada para clientes associados a este ponto de acesso. A taxa deve estar entre 0 e 86400, com um valor 0 desabilitando o recurso.

Broadcast Key Refresh Rate: ?


86400

Note: Neste exemplo, 86400 é usado.

Etapa 11. Escolha uma opção na lista suspensa MFP se você deseja que o WAP exija ter quadros protegidos ou não. Para saber mais sobre o MFP, clique [aqui](#). As opções são:

- Não obrigatório — Desativa o suporte ao cliente para MFP.

- Capable (Capaz) — Permite que clientes compatíveis com MFP e que não suportam MFP entrem na rede. Essa é a configuração MFP padrão no WAP.
- Obrigatório — Os clientes podem se associar somente se o MFP for negociado. Se os dispositivos não oferecerem suporte a MFP, eles não poderão ingressar na rede.

Broadcast Key Refresh Rate: 


MFP:

Note: Para este exemplo, Capable é escolhido.


Etapa 12. Clique em **OK** para salvar as configurações de segurança.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES


Key: 

Show Key as Clear Text

Broadcast Key Refresh Rate: 

MFP:

A área Status da conexão indica Não aplicável ou N/A.

Encryption	Connection Status
WPA Personal	Disconnected
<input type="text" value="WPA Personal"/> 	<input type="text" value="N/A"/>

Etapa 13. Digite o ID da VLAN no campo ID da VLAN para a interface do ponto de acesso.

Note: Para permitir o bridging de pacotes, a configuração da VLAN para a interface do ponto de acesso e a interface com fio deve corresponder à da interface do cliente de infraestrutura.

N/A	<input type="text" value="1"/>	<input checked="" type="checkbox"/>
-----	--------------------------------	-------------------------------------

Etapa 14. Marque a caixa de seleção SSID Broadcast (Transmissão de SSID) se desejar que o SSID de downstream seja transmitido. SSID Broadcast (Transmissão de SSID) está ativado por padrão.

VLAN ID	SSID Broadcast	Client Filter
1	N/A	N/A

<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Disabled
--------------------------------	-------------------------------------	----------

Etapa 15. Escolha o tipo de filtragem MAC que deseja configurar para a interface do ponto de acesso na lista suspensa Filtragem MAC. Quando habilitados, os usuários recebem ou negam acesso ao WAP com base no endereço MAC do cliente que usam.

As opções disponíveis são definidas da seguinte forma:

- Desabilitado — Todos os clientes podem acessar a rede upstream. Este é o valor padrão.
- Local — O conjunto de clientes que podem acessar a rede upstream é restrito aos clientes especificados em uma lista de endereços MAC definidos localmente.
- RADIUS — O conjunto de clientes que podem acessar a rede upstream é restrito aos clientes especificados em uma lista de endereços MAC em um servidor RADIUS.

Note: Neste exemplo, Desabilitado é escolhido.

Etapa 16. Clique em **Salvar** para salvar suas alterações.

Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	1	N/A	N/A

N/A	<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Disabled
-----	--------------------------------	-------------------------------------	----------

Agora você deve ter configurado com êxito as configurações da ligação do grupo de trabalho em seus pontos de acesso sem fio.